Статью рекомендовал к опубликованию к.т.н. Г.В. Карайчев.

Тенетко Михаил Иванович
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: tenetko@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 88622535982.
Независимый специалист.

Пескова Ольга Юрьевна
E-mail: poy@tsure.ru.
Тел.: 88634371905.
К.т.н.; доцент.

Tenetko Mikhail Ivanovich
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: tenetko@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: +78622535982.
Independent Specialist.

Peskova Olga Yur’evna
E-mail: poy@tsure.ru.
Phone: +78634371905.
Cand. of Eng. Sc.; Associate Professor.

УДК 004.056.5, 004.89

А.М. Цыбулин

АРХИТЕКТУРА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Количество атак на информационные системы предприятий неуклонно растет. В связи с этим возрастают количество анализируемых событий безопасности, разнообразие механизмов защиты, а также вероятности ошибок при конфигурировании аппаратного, программного обеспечения и анализе инцидентов безопасности. Целью исследования является разработка архитектуры автоматизированной системы управления информационной безопасностью предприятия. Использование автоматизированной системы управления позволяет разрешить указанные проблемы за счет решения следующих задач: автоматизация централизованного и децентрализованного мониторинга и аудита управления информационной безопасностью, синтез оптимального решения по повышению уровня информационной безопасности для предприятия.

Атака, интеллектуальный агент; многоагентная система; информационная безопасность; управление информационной безопасностью; мониторинг; аудит; катастрофоустойчивость; информационная система.

A.M. Tsybulin

AUTOMATED INFORMATION SECURITY MANAGEMENT SYSTEM OF ENTERPRISE ARCHITECTURE

The total amount of attacks on enterprise’s information system more and more increases. Therefore analyzed security events, security incidents, the variety of security mechanisms and also error’s probability during hardware’s and software’s configuration are increased too. The main

goal of the research is the developing the architecture of enterprise's information security management. Using automated management system allows us to remedy pointed questions by solving following tasks: automation of centralized and decentralized monitoring and audit of information security management, making optimal decision for improving the level of enterprise's information security.

Attack; intelligent agent; multi-agent system; information security; information security management; monitoring; audit; disaster tolerance; information system.

Практика эксплуатации информационных систем подтверждает, что злоумышленные действия над информацией не только не прекращаются, а имеют достаточно устойчивую тенденцию к росту. Для успешного противодействия этой тенденции уже недостаточно стройной и управляемой системы обеспечения безопасности информации, созданной уникальными системными администраторами или специалистами по защите информации на основе своего опыта и интуиции. В работе они сталкиваются с современными проблемами информационной безопасности (ИБ).

Первая проблема. Большое количество разнородных механизмов и мероприятий безопасности:

- 90 % используют межсетевые экраны и антивирусы;
- 40 % используют системы обнаружения вторжений (СОА);
- количество сетевых устройств растет;
- большое количество организационных мероприятий по информационной безопасности;
- больше оборудования и мероприятий, означает большую сложность.

Вторая проблема. Резкое увеличение событий безопасности:

- один межсетевой экран может генерировать за день более 1 Гигабайта данных в Log-файле;
- один сенсор СОА за день может выдавать до 50 тыс. сообщений, до 95 % ложных тревог;
- сопоставить сигналы безопасности от разных систем безопасности практически невозможно.

Третья проблема, являющаяся следствием первой и второй проблем – существенное увеличение вероятности ошибок при конфигурировании аппаратного и программного обеспечения и анализе инцидентов безопасности в современных информационных систем (ИС) в ограниченное время.

Разрешение этих проблем, возможно только за счет автоматизации процессов управления информационной безопасностью предприятия, т.е. создании единой системы поддержки принятия решений, нацеленных на нормализацию функционирования информационной системы предприятия.

При этом требуется решить две задачи. Во-первых необходимо обеспечить централизованное накопление и постоянное обновление актуальных знаний обо всех бизнес-процессах предприятия, связанных не только с информационной безопасностью. Во-вторых, нужно организовать обработку этой информации в автоматическом или автоматизированном режиме и генерирование возможных управляющих воздействий.

Для решения первой задачи предлагается использовать единое информационное пространство предприятия. Организация единого информационного пространства в соответствии с современными тенденциями развития информационных технологий состоит в интеграции всех информационных ресурсов предприятия. При этом происходит внедрение автоматизированных систем с различной функциональностью, разработка нового программного обеспечения и активное использование современных технологий обеспечения информационной безопасности на предприятии.

Управление процессом обеспечения информационной безопасности основано на решении следующих задач:

- сбор данных от различных подсистем обеспечения информационной безопасности (мониторинг);
- автоматизация анализа (аудит)и хранения событий безопасности;
- обработка инцидентов ИБ и выработка управляющих воздействий;
- автоматизированное управление системой информационной безопасности из единого центра;
- автоматизированная генерация отчетов различной степени детализации для руководителей и специалистов;
- хранение в структурированном виде и актуальных документов по информационной безопасности организации, базы событий, инцидентов и рисков ИБ, перечней активов и прочее в едином информационном пространстве.

Комплексное решение указанных задач невозможно без построения автоматизированной системы управления (АСУ) информационной безопасности предприятия (ИБП).

Для обоснования управленческих решений и оценки их эффективности в силу сложности бизнес-процессов предприятия используются оценки рисков.

При построении системы безопасности предприятия обеспечивается управление рисками, а именно: определение рисков, выработка мероприятия по снижению рисков и создание системы безопасности, при которой риски будут находиться в приемлемом (допустимом) состоянии. На практике используются и другие критерии, построенные на базе рисков.

Уровень защищенности информации определяется через относительный риск [1]:

$$\psi = (1 - P * C / C_{\Sigma}), \quad (1)$$

где – ψ относительный риск; C – суммарная ценность защищаемых информационных ресурсов в ИС; P – результирующая вероятность реализации множества угроз информационной системе, со структурой системы защиты информации S; C_{Σ} – суммарный неприемлемый ущерб. Отношение C/C_{Σ} – коэффициент опасности совокупности угроз ИС.

Для формализации процессов управления безопасностью по критерию (1), предлагается следующая модель.

Определим множество информационных объектов в информационной системе:

$$O=\{O_1,O_2,\ldots,O_n\}, \quad (2)$$

где n – количество всех информационных объектов.

Каждый информационный объект описывается совокупностью атрибутов A_{Oi} и связей R_{Oi}, т.е. все информационное пространство предприятия представляет собой семантическую сеть.

Совокупность информационных объектов также является информационным объектом. В связи с чем, набор уровней защищенности имеет смысл задавать для информационного объекта следующим образом:

$$\boldsymbol{R_{Oi}}=\{\psi_i = (\boldsymbol{p_i}, \boldsymbol{c_i}, \boldsymbol{t_i})\}, \quad (3)$$

где i = 1,…,I, I – количество всех предусмотренных уровней защищенности объекта;

$\boldsymbol{p_i}$ – вероятность наступления риска для i-го объекта;

$\boldsymbol{c_i}$ – ущерб в результате наступления риска для i-го объекта (измеряется в условных единицах);

$\boldsymbol{t_i}$ – время выявления изменения риска для i-го объекта.

Атрибуты $\boldsymbol{A_i}=\{a_{i1},a_{i2},\ldots,a_{ik}\}$ – множество параметров настройки механизмов и мер защиты i-го объекта, k – мощность множества параметров.

Как любая система управления с позиций кибернетического подхода АСУ ИБП должна включать в себя управляющую систему (УС), объект управления (ОбУ), систему защиты информации (СЗИ) и систему связи.

В кибернетике используется принцип дуальности, который утверждает, что **информация, необходимая для управления** некоторым объектом, добывается с использованием **средств наблюдения** объекта в ходе управления. Этот принцип утверждает необходимость **обратной связи** в системе управления [2].

В рассматриваемом случае, объект управления – современная система защиты информации является сложной системой. Например, СЗИ распределенной, территориально-разнесенной информационной системы предприятия. Эта СЗИ не может управляться каким-либо единым центром. СЗИ требует распределенных подсистем управления, принимающих самостоятельные решения на основе знаний и механизмов логического вывода [3]. Такие подсистемы образуют некоторое сообщество, в котором они объединяются общими целями и используют множество ограниченных ресурсов для достижения этих целей. Это способствовало возникновению и развитию многоагентных систем, реализующих совместную деятельность множества интеллектуальных агентов по достижению общей цели [4].

В соответствии с этим совокупность функций управления в АСУ ИБП составляет множество циклов управления при изменении относительных рисков для множества информационных объектов. При этом интеллектуальный агент мониторинга и аудита (агент МиА) на основе своей базы знаний, данных от своих сенсоров контроля трафика, перехвата последовательности системных вызовов, журналов безопасности определяет пути дальнейшего развития деструктивного воздействия (атаки) и рассчитывает текущий относительный риск ψ_i для i-го информационного объекта. Интеллектуальный агент моделирующий управляющую подсистему (агент УСП) i-го информационного объекта располагает знаниями об его атрибутах A_{Oi} и связях R_{Oi}, которые отражают текущее состояние защищенности объекта.

Агент УСП для реализации своей цели управления анализирует на основе данных от агента мониторинга и аудита (МА) отклонение текущего значения относительного риска ψ_i от требуемого и определяет необходимость изменения текущего состояния. По результатам анализа вырабатывается **решение** либо по удержанию атрибутов информационного объекта в текущем состоянии, либо по их изменению и перевода объекта управления в новое состояние. Решение о переводе объекта в новое состояние вырабатывается также в случае корректировки цели управления ЗИ, которая определяется заданием требуемого значения уровня защищенности. Эти решения в виде сообщения передаются агенту ОбУ, который их реализует путем пошаговой корректировки множества атрибутов A_{Oi} настройки механизмов и мер защиты *i*-го объекта и связей R_{Oi}, в соответствии со сценариями действий, располагаемыми в его базе знаний. Действия агентов МиА, УСП и ОбУ протоколируются в базе данных с привязкой к времени. Рассмотренные компоненты АСУ ИБП погружены в информационную систему предприятия. Объектами управления АСУ ИБП являются механизмы защиты информационных объектов. Архитектура АСУ ИБП приведена на рисунке.

Модель целей управления в виде дерева целей агентов для каждого информационного объекта строится в соответствии со стратегическими и оперативными целями функционирования предприятия на основании ряда правил [5]. Например, достижение пяти целей управления, позволяет минимизировать относительный риск информационной безопасности:

- минимизация несанкционированного доступа к информационным объектам;
- защита от вредоносного программного обеспечения (ПО);

- рациональное использование внутреннего трафика;
- рациональное использование внешнего трафика;
- рациональное конфигурирование аппаратного и программного обеспечения.

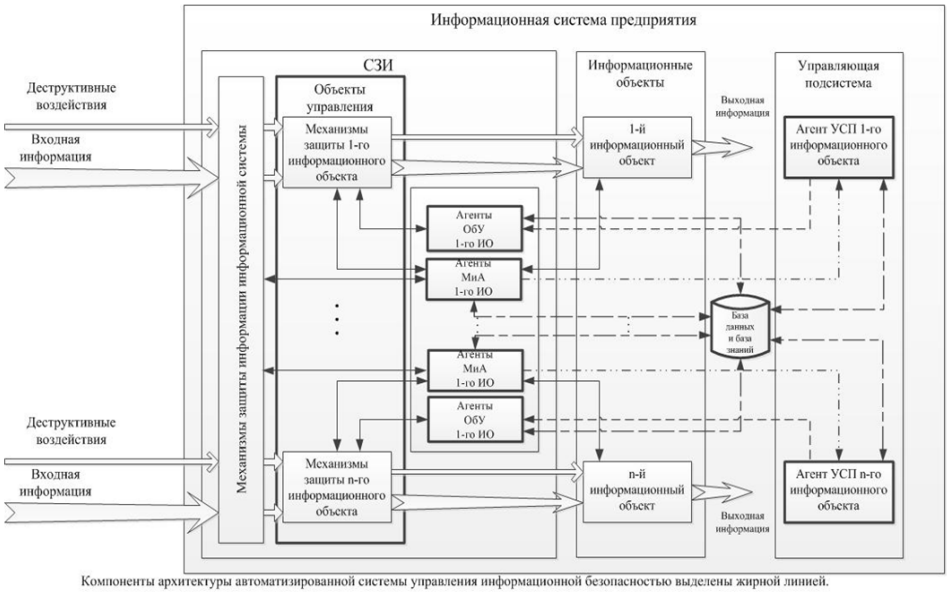

Рис. Архитектура автоматизированнлй системы управления информационной безопасностью предприятия

Дерево целей для автоматизированной системы управления, приведено в таблице.

Таблица

Дерево целей для автоматизированной системы управления

Номер узла	Описание цели
0.	Минимизация остаточного риска информационной безопасности
1.	Минимизация несанкционированного доступа к информационным ресурсам
1.1.	Минимизация числа попыток доступа к информационным ресурсам (ИО) с неавторизованных рабочих мест
1.2.	Минимизация числа попыток доступа к ИО неавторизованным ПО
1.3.	Минимизация числа прочих попыток несанкционированного доступа к ИО
1.3.1.	Минимизация числа попыток перебора и подбора паролей
1.3.2.	Минимизация числа попыток применения эксплоитов и атак на ИО
1.4.	Минимизация числа нарушений регламента работы с ИО
1.4.1.	Минимизация числа нарушений правил эксплуатации ИО
1.4.2.	Минимизация случаев вмешательства в работу ИО и прикладного ПО для доступа к ИО
1.4.2.1	Обнаружение умышленного вмешательства
1.4.2.2.	Обнаружение неумышленного вмешательства (установка несовместимого ПО и т.п.)
2.	Защита от вредоносного ПО
2.1.	Исключение вредоносных программ на ЭВМ пользователей

Окончание табл.

Номер узла	Описание цели
2.2.	Исключение потенциально опасных и запрещенных программ
2.3.	Исключение сбоев в работе антивируса и вмешательства в его работу
2.3.1.	Исключение сбоев по вине пользователя
2.3.2.	Исключение сбоев по причине активного заражения компьютера вирусами
2.3.3.	Исключение сбоев по техническим причинам, не зависящим от пользователя
3.	Рациональное использование внутреннего трафика
3.1.	Минимизация аномалий в локальном трафике корпоративной вычислительной сети (КВС)
3.2.	Минимизация самовольных подключений сетевых устройств к ЭВМ или КВС
3.3.	Минимизация самовольного изменения сетевых настроек
4.	Рациональное использование внешнего трафика.
4.1.	Минимизация аномалий и нарушений работы Интернета и борьба с ними
4.2.	Своевременное обнаружение аномалий и нарушений в работе электронной почты и борьба с ними
5	Рациональное конфигурирование аппаратного и программного обеспечения
5.1.	Минимизация случаев самовольной установки ПО
5.2.	Минимизация случаев самовольного изменения аппаратной

В настоящее время проводятся исследования модели автоматизированной системы управления информационной безопасностью предприятия с целью отладки и расширения дерева целей управления.

Практическая значимость. Повышение эффективности защиты данных в информационных системах предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Машкина И.В.* Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий: Дис. … д-ра техн. наук. – Уфа: Изд-во ГОУ ВПО Уфимский государственный авиационный технический университет, 2009. – 332 с.
2. *Анфилатов В.С.* Системный анализ в управлении: Учебное пособие / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин / Под ред. А.А. Емельянова. – М.: Финансы и статистика, 2006 . – 368 с.
3. *Емельянов В.В.* Имитационное моделирование систем: Учебное пособие / Емельянов В.В., Ясиновский С.И. – М.: Изд-во МГТУ им. Баумана, 2009. – 584 с.
4. *Цыбулин А.М., Никишова А.В., Умницын М.Ю.* Исследование противоборства службы безопасности и злоумышленников на многоагентной модели // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 94-99.
5. *Стоянова О.В., Зайцев О.В.* Метод дерева целей для оценки эффективности использования информационных ресурсов // Программные продукты и системы. – 2009. – № 3.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Цыбулин Анатолий Михайлович
Федеральное государственное бюджетне образовательное учреждение высшего профессионального образования «Волгоградский государственный университет».
E-mail: anatsybulin@yandex.ru.
400062, г. Волгоград, пр. Университетский, 100.
Тел.: 88442460368.
Зав. кафедрой информационной безопасности.

Tsybulin Anatoly Mihaylovich
Volgograd State University.
E-mail: anatsybulin@yandex.ru.
100, Universitetsky Pr., Volgograd, 400062, Russia.
Phone: +78442460368.
Head of Department of Information Security.

УДК 004.056.5

В.Г. Миронова, А.А. Шелупанов

СЕТИ ПЕТРИ КАК ИНСТРУМЕНТ АНАЛИЗА СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Построение системы защиты является обязательным условием для обеспечения безопасности конфиденциальной информации, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования информационной системы и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищенности системы является построение раскрашенных сетей Петри. С помощью аппарата сетей Петри проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки.

Система защиты конфиденциальной информации; информационная система; сети Петри.

V.G. Mironova, A.A. Shelupanov

PETRI NETS AS A TOOL FOR THE ANALYSIS OF THE PROTECTION CONFIDENTIAL INFORMATION

Building security is a prerequisite for the security of confidential information stored and processed in the information system. System requirements of information security are formed based on the results of the survey and information system aimed at neutralizing the vulnerabilities of the system. One way of security analysis system is the construction of colored Petri nets. With the help of Petri nets functioning of the survey is conducted of the implemented system security and identify its weaknesses.

System to protect confidential information; information system; Petri net.

Развитие информационных систем обработки и хранения конфиденциальной информации диктует необходимость построения надежной системы защиты конфиденциальной информации (СЗКИ).

Построение СЗКИ проводится в несколько этапов. Первым этапом является обследование информационной системы (ИС), в рамках которого анализируется технология обработки, хранения и защиты информации, формируется модель нарушителя и модель угроз безопасности конфиденциальной информации (КИ), а также составляются требования к СЗКИ.